IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-5, Issue-4 E-ISSN: 2347-2693

Cloud Security Threats and Issues-A Review

R. Sood[1*], R. Sharma[2]

[1]Computer Science and Engineering, CGC College of Engineering (PTU Jalandhar), Mohali, India
[2] Computer Science and Engineering, CGC College of Engineering, (PTU Jalandhar), Mohali, India

Corresponding Author: reecha.coecse@cgc.edu.in
www.ijcseonline.org

Received: 02/Mar/2017, Revised: 14/Mar/2017, Accepted: 14/Apr/2017, Published: 30/Apr/2017

Abstract: Cloud Computing is one of the best on-demand network access service available to a large shared pool of computing resources in today's world. There are various economic benefits of cloud computing which are widely recognized. Cloud computing help users to avail benefits of having large storage (IAAS), variety of OS (PAAS) and other softwares (SAAS) at their premises without the need to have them at their own hardware level. Apart from these economic benefits, public clouds still haven't seen widespread adoption, especially by enterprises. Most large organizations today run private clouds, in the sense of virtualized and geographically distributed data centers, but rarely rely primarily on externally managed resources. Major reason behind this is the security concerns involved in existing cloud infrastructures which includes hardware failures, software bugs, power outrages, server miniconfiguration, malware and inside threats. The aim of this paper is to throw light on various Cloud security threats and issues as well as security issues inherent within the context of cloud computing and cloud infrastructure.

***Keywords*—**IAAS, PAAS, SAAS Multi-Tenancy, Orchestratio

1. INTRODUCTION

Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology.

With the introduction of numerous clouds based services and geographically dispersed cloud service providers, sensitive information of different entities belonging to different origin are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. This paper presents a review on the cloud computing concepts as well as security issues and the threats inherent within the context of cloud computing and cloud infrastructure.

One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud.

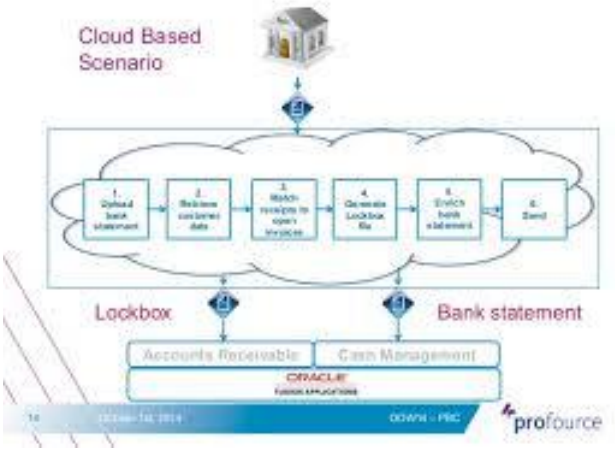


Figure 1 illustrates a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud

Cloud Computing is a technique which provides flexibility, anytime anywhere any resource & mobility (i.e. on the go) facilities to its users, thereby increasing their profits. It acquires a large number of users which require either infrastructure (i.e. servers, Disk space, bandwidth etc. IAAS) or platform (such as OS i.e. PAAS) or some licensed softwares (i.e. SAAS).
Cloud computing is typically classified in three ways namely:
i. Public Cloud
ii. Private Cloud
iii. Hybrid Cloud

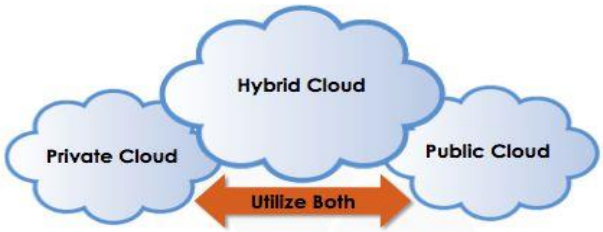


Figure 2 illustrates the different types of clouds available.

Type of Cloud	Description
Public Cloud	Computing Infrastructure is at vendor's premises and is not visible to the user. Moreover, user doesn't have any control over computing infrastructure, which is shared between organizations.
Private Cloud	Computing infrastructure is dedicated to the particular organization and is not shared with other organization. Private clouds are more expensive and more secured.
Hybrid Cloud	Being the combination of both the public and private cloud, hybrid cloud enjoys the advantages of both.

However security concerns put obstructions in the path of users to adopt cloud computing. As the center security element, authentication plays a vital role in an advanced computing model. So, identity theft still is one of the most predominant issues in the cloud systems. In the past, confidential data stored on PC and the computer itself was physically protected & authenticity was checked physically as well as by using username and passwords. However in today's world of cloud computing since the data is stored at third party's server where physical security is not possible, moreover username & passwords can also be hacked. In such a scenario securing your data is the biggest concern. The most recognized model of cloud computing too many consumers is public cloud, where services are provided in a virtual environment using shared physical resources and accessible over the public network such as internet. The most important challenge to security of public cloud is confidentiality of its sensitive data

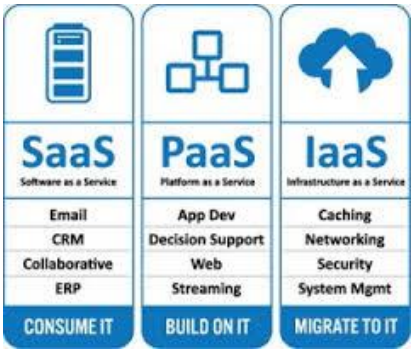


Figure 3 illustrates the basic applications of IAAS, PAAS, and SAAS

COMPARISION BETWEEN CLOUD AND GRID COMPUTING

A comparison can be summaries as follows:
1) Construction of the grid is to complete a specified task, such as biology grid, Geography grid, national educational grid, while Cloud computing is designed to meet general application and there are not grid for a special field.
2) Grid emphasizes the "resource sharing" to form a virtual organization. Cloud is often owned by a single physical organization (except the community Cloud, in this case, it is owned by the community), who allocates resources to different running instances.
3) Grid aims to provide the maximum computing capacity for a huge task through resource sharing. Cloud aims to suffice as many small-to-medium tasks as possible based on users' real-time requirements. Therefore, multi-tenancy is a very important concept for Cloud computing.
4) Grid trades re-usability for (scientific) high performance computing. Cloud computing is directly pulled by immediate user needs driven by various business requirements.
5) Grid strives to achieve maximum computing. Cloud is after on-demand computing – Scale up and down, in and out at the same time optimizing the overall computing capacity.

2. THREATS TO CLOUD COMPUTING

1 Data breaches

The severity of potential damage tends to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more dangerous.

When a data theft occurs, companies may incur fines, or they may face criminal charges. Breach investigations and customer notifications can rack up significant costs. Indirect effects, such as brand damage and loss of business, can impact organizations for years.

Cloud providers typically deploy security controls to protect their environments, but ultimately, organizations are responsible for protecting their own data in the cloud. The CSA has recommended organizations use multifactor authentication and encryption techniques to protect against data breaches and thefts.

2: COMPROMISED CREDENTIALS AND BROKEN AUTHENTICATION

Data breaches and other attacks frequently result from lax authentication, weak passwords, and poor key or certificate management. Organizations often struggle with identity management as they try to allocate permissions appropriate to the user's job role.

Multifactor authentication systems such as one-time passwords, phone-based authentication, and smartcards protect cloud services because they make it harder for attackers to log in with stolen passwords.

Many developers make the mistake of embedding credentials and cryptographic keys in source code and leaving them in public-facing repositories such as GitHub. Keys need to be appropriately protected, and a well-secured public key infrastructure is necessary, the CSA said. They also need to be rotated periodically to make it harder for attackers to use keys they've obtained without authorization.

3: HACKED INTERFACES AND APIS

Practically every cloud service and application now offers APIs. IT teams use interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management, orchestration, and monitoring.

The security and availability of cloud services -- from authentication and access control to encryption and activity monitoring -- depend on the security of the API. Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability.

APIs and interfaces tend to be the most exposed part of a system because they're usually accessible from the open Internet. The CSA recommends adequate controls as the "first line of defense and detection."The CSA also recommends security-focused code reviews and rigorous penetration testing.

4: EXPLOITED SYSTEM VULNERABILITIES

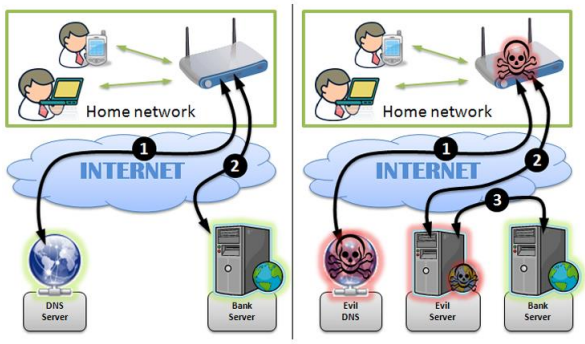
System vulnerabilities, or exploitable bugs in programs, are not new, but they've become a bigger problem with the advent of multitenancy in cloud computing. Organizations share memory, databases, and other resources in close proximity to one another, creating new attack surfaces.

According to the CSA, the costs of mitigating system vulnerabilities "are relatively small compared to other IT expenditures." The expense of putting IT processes in place to discover and repair vulnerabilities is small compared to the potential damage. Change control processes that address emergency patching ensure that remediation activities are properly documented and reviewed by technical teams.

5: ACCOUNT HIJACKING

Phishing, fraud, and software exploits are still successful, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may also be able to use the cloud application to launch other attacks.

Figure 4 illustrates hijacking



Common defense-in-depth protection strategies can contain the damage incurred by a breach. Organizations should prohibit the sharing of account credentials between users and services, as well as enable multifactor authentication schemes where available. Accounts, even service accounts, should be monitored so that every transaction can be traced to a human owner.

6: MALICIOUS INSIDERS

The insider threat has many faces: a current or former employee, a system administrator, a contractor, or a business

partner. The malicious agenda ranges from data theft to revenge. In a cloud scenario, a hellbent insider can destroy whole infrastructures or manipulate data. Systems that depend solely on the cloud service provider for security, such as encryption, are at greatest risk.

The CSA recommends that organizations control the encryption process and keys, segregating duties and minimizing access given to users. Effective logging, monitoring, and auditing administrator activities are also critical. As the CSA notes, it's easy to misconstrue a bungling attempt to perform a routine job as "malicious" insider activity. Proper training and management to prevent such mistakes becomes more critical in the cloud, due to greater potential exposure.

7: THE APT PARASITE

The CSA aptly calls advanced persistent threats (APTs) "parasitical" forms of attack. APTs infiltrate systems to establish a foothold, then stealthily exfiltrate data and intellectual property over an extended period of time.

APTs typically move laterally through the network and blend in with normal traffic, so they're difficult to detect. The major cloud providers apply advanced techniques to prevent APTs from infiltrating their infrastructure, but customers need to be as diligent in detecting APT compromises in cloud accounts as they would in on-premises systems.

In particular, the CSA recommends training users to recognize phishing techniques. Regularly reinforced awareness programs keep users alert and less likely to be tricked into letting an APT into the network -- and IT departments need to stay informed of the latest advanced attacks. Advanced security controls, process management, incident response plans, and IT staff training all lead to increased security budgets. Organizations should weigh these costs against the potential economic damage inflicted by successful APT attacks.

8: PERMANENT DATA LOSS

As the cloud has matured, reports of permanent data loss due to provider error have become extremely rare. But malicious hackers have been known to permanently delete cloud data to harm businesses, and cloud data centers are as vulnerable to natural disasters as any facility. Cloud providers recommend distributing data and applications across multiple zones for added protection. Adequate data backup measures are essential, as well as adhering to best practices in business continuity and disaster recovery. Daily data backup and off-site storage remain important with cloud environments.

The burden of preventing data loss is not all on the cloud service provider. If a customer encrypts data before uploading it to the cloud, then that customer must be careful to protect the encryption key. Once the key is lost, so is the data. Compliance policies often stipulate how long organizations must retain audit records and other documents. Losing such data may have serious regulatory consequences.

9: INADEQUATE DILIGENCE

Organizations that embrace the cloud without fully understanding the environment and its associated risks may encounter a "myriad of commercial, financial, technical, legal, and compliance risks," the CSA warned. Due diligence applies whether the organization is trying to migrate to the cloud or merging (or working) with another company in the cloud. For example, organizations that fail to scrutinize a contract may not be aware of the provider's liability in case of data loss or breach.

Operational and architectural issues arise if a company's development team lacks familiarity with cloud technologies as apps are deployed to a particular cloud. The CSA reminds organizations they must perform extensive due diligence to understand the risks they assume when they subscribe to each cloud service.

10: CLOUD SERVICE ABUSES

Cloud services can be commandeered to support nefarious activities, such as using cloud computing resources to break an encryption key in order to launch an attack. Other examples including launching DDoS attacks, sending spam and phishing emails, and hosting malicious content.

Providers need to recognize types of abuse -- such as scrutinizing traffic to recognize DDoS attacks -- and offer tools for customers to monitor the health of their cloud environments. Customers should make sure providers offer a mechanism for reporting abuse. Although customers may not be direct prey for malicious actions, cloud service abuse can still result in service availability issues and data loss.

11: DOS ATTACKS

DoS attacks have been around for years, but they've gained prominence again thanks to cloud computing because they often affect availability. Systems may slow to a crawl or simply time out. "Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock; there is one way to get to your destination and there is nothing you can do about it except sit and wait," the report said.

DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. While high-volume DDoS attacks are very common, organizations should be aware of asymmetric, application-level DoS attacks, which target Web server and database vulnerabilities.

12: SHARED TECHNOLOGY, SHARED DANGERS

Vulnerabilities in shared technology pose a significant threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone.

If an integral component gets compromised -- say a hypervisor, a shared platform component, or an application -- it exposes the entire environment to potential compromise and breach.

REFERENCES

[1]. A.A. Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, Deqing Zou, "*Efficient Password based Two Factors Authentication in Cloud Computing*", International Journal of Security and Its Applications, Vol. 6, No. 2 , pp.143-148, 2012

[2]. S. Renu, OHH Parveen, "*Biometric Based Approach for Data Sharing in Public Cloud*", International Journal of Advanced Research in Computer and Communication Engineering Vol.4, Issue.2 pp.1-9, 2015

[3]. Mithilesh Mittal, Pradeep Sharma and Pankaj Kumar Gehlot, "*A Comparative Study of Security Issues& Challenges of Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.5, pp.9-15, 2013.

[4]. Vivek Raich, Pradeep Sharma, Shivlal Mewada and Makhan Kumbhkar, "*Performance Improvement of Software as a Service and Platform as a Service in Cloud Computing Solution*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.6, pp.13-16, 2013.

[5]. R. Buyyaa, C. S. Yeoa, S. Venugopala, J. Broberg, I. Brandic, "*Cloud Computing and Emerging IT platforms: Vision Hype and Reality for Delivering Computing as the 5th Utility*", Future Generation Computer Systems, Vol.25, Issue.6, pp. 599-616, 2009.

[6]. W. Publishing, J. Wiley, B.Sosinsky, "*Cloud Computing Bible*" Published by Wiley Publishing, US, pp.1-480, 2010.

[7]. S. Shukla, D. kumar, "*Clouds Software- Security as a Service(S-SaaS) via Biometrics*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.119-124, 2014.

[8]. N. Mead, et ai, "*Security quality requirements engineering (SQUARE) methodolgy*", ACM SIGSOFT Software Engineering, Vol.30 Issue.4, pp.1-7, 2005

[9]. JW. Rittinghouse, JF. Ransome, "Cloud Computing", Taylor and Francis Group, US, pp.1-284, 2010.

[10]. A. Bansal, A. Agrawal, "*Providing Confidentiality, Integrity and Atomicity for data stored in the cloud storage*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.10, pp.65-70, 2016.

[11]. Rakesh Prasad Sarang and Rajesh Kumar Bunkar, "*Study of Services and Privacy Usage in Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.6, pp.7-12, 2013.

[12]. V.K. Saxena, S. Pushkar, "*Privacy Preserving using Encryption Proxy in Data Security*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.2, pp.36-41, 2017.

